II. CLAIM AMENDMENTS

1-5. (Cancelled)

6. (Previously Presented) A method to authenticate a mobile station in a mobile network comprising:

authenticating the mobile station with user-to-user data exchange;

exchanging authentication data during call set-up or during a call;

wherein an encryption key is agreed between two mobile stations and the mobile stations execute a mutual authentication and key agreement protocol based on public-key cryptography and,

wherein a second mobile station is authenticated by:

a first mobile station constructing and sending to the second mobile station a first message, the second mobile station receiving the first message,

constructing and sending a second message to the first mobile station,

the first mobile station receiving the second message, checking the validity of the information in the second message, if the information is verified valid the first mobile station accepting to share a shared encryption key K with the second mobile station, the first mobile station constructing and sending a third message to the second mobile station,

the second mobile station receiving the third message and verifying the validity of the information, if the information is valid the second mobile station accepting the sharing of the shared encryption key K with the first mobile station.

7. (Previously Presented) A method to authenticate a mobile station in a mobile network comprising:

authenticating the mobile station with user-to-user data exchange;

an encryption key is agreed between two mobile stations;

the two mobile stations execute a mutual authentication and key agreement protocol based on public key cryptography;

the second mobile station is authenticated by:

a first mobile station constructing and sending to the second mobile station a first message, the second mobile station receiving the first message,

constructing and sending a second message to the first mobile station,

the first mobile station receiving the second message, checking the validity of the information in the second message, if the information is verified valid the first mobile station accepting to share a shared encryption key K with the second mobile station, the first mobile station constructing and sending a third message to the second mobile station,

the second mobile station receiving the third message and verifying the validity of the information, if the information is valid the second mobile station accepting the sharing of the shared encryption key K with the first mobile station,

the second mobile station is authenticated by the first mobile station selecting a prime number p, a generator a of a multiplicative group of integers modulo p when $p \geq a \geq 2$ and a random secret x when $p-2 \geq x \geq 1$, constructing and sending to the second mobile station the first message containing

$$a, p, a^x \bmod p,$$

the second mobile station receiving the first message and afterwards generating a secret y when $p-2 \geq y \geq 1$ and computing a second shared key $K_2 = (a^x)^y \bmod p$, signing a concatenation of exponentials $\{a^y, a^x\}$ and encrypting a result $S_B\{a^y, a^x\}$

with the second shared key leading to $E_K(S_B\{a^y, a^x\})$, constructing and sending the second message to the first mobile station containing

$$a^y \bmod p, cert_B, E_K(S_B\{a^y, a^x\}),$$

certificate $cert_B$ in the second message containing a signature verification key of the second mobile station, the exact contents of the certificate being of at least the following minimum

$$cert_B = (B, p_B, a, p, S_T\{B, p_B, a, p\}),$$

p_B being a public signature verification key of the mobile station B and S_T a signature transformation of a trusted authority T whose public signature verification key is known in the first and second mobile stations,

the first mobile station receiving the second message and afterwards computing a first shared encryption key $(a^y)^x \bmod p = (a^x)^y \bmod p = K_1$, checking the validity of the certificate $cert_B$ the first mobile station, when the certificate $cert_B$ is valid the encrypted part $E_K(S_B\{a^y, a^x\})$ of the second message is decrypted to receive a signature $S_B\{a^y, a^x\}$ and the signature $S_B\{a^y, a^x\}$ is verified with a public signature verification key p_B of the second mobile station, if the signature $S_B\{a^y, a^x\}$ is verified valid the first mobile station accepts to share the shared encryption key K_1 with the second mobile station,

the first mobile station signing a concatenation of exponentials $\{a^x, a^y\}$ and encrypting result $S_A\{a^x, a^y\}$ with the first shared key K_1 leading to $E_K(S_A\{a^x, a^y\})$, the first mobile station constructing and sending the third message to the second mobile station containing

$$cert_A, E_K(S_A\{a^x, a^y\}),$$

$cert_A$ including corresponding information with $cert_B$ of the first mobile station, exact contents of the certificate $cert_A$ being at least of the following minimum

$$cert_A = (B, p_A, a, p, S_T\{B, p_A, a, p\}),$$

p_A being a public signature verification key of the first subscriber and S_T a signature transformation of a trusted authority T whose public signature verification key is known by the first and second mobile stations,

the second mobile station receiving the third message and verifying validity of the $cert_A$, decrypting $E_A(S_A\{a^x, a^y\})$ and verifying validity of signature of $S_A\{a^x, a^y\}$, if all the signatures are valid the second mobile station accepting sharing of the second shared encryption key K_2 with the mobile station.

8. (Cancelled)

9. (Previously Presented) A cellular communications system, where the first and second mobile stations are wireless connected with via base stations, wherein the system comprises

a) a first mobile station, authenticated with user-to-user data exchange during call set up or during a call, that constructs and sends a first message, receives and verifies the validity of a second message and when the information is verified valid accepts to share a shared encryption key K, constructs and sends a third message,

b) a second mobile station, that receives the first message and constructs and sends the second message, receives and verifies the validity of the third message and when the information is valid accepts to share the shared encryption key K with the first mobile station, and

c) at least one mobile switching centre.

10. (Previously Presented) A communications system according to claim 9, wherein the system comprises two mobile switching centres connected together with ISDN.

11. (Previously Presented) A mobile station, wherein the mobile station comprises:

a) a processor to perform operations needed to form and verify messages, to implement authentication of the mobile station with user-to-user data exchange during call set up or during a call, and key agreement procedures,

b) a memory, where procedures and messages are stored with necessary parameters and variables,

c) output means, on which commencement of extra secure communication is presented to a user of the mobile station,

d) input means to enable validation of the extra secure communication,

e) a transmitter/receiver and an antenna to transform information to radio waves from digital signals and vice versa.

12. (Previously Presented) A mobile station according to claim 11, wherein the output means comprises a display.

13. (Previously Presented) A mobile station according to claim 11,wherein the input means comprises a keyboard.

14. (Previously Presented) A mobile station according to claim 11, wherein the mobile station is designed to GSM standards.

15. (Previously Presented) A mobile station according to claim 11, wherein the mobile station is designed to UTMS standards.

16. (Previously Presented) A method to authenticate a mobile station in a mobile network, wherein a first mobile station and a second mobile station are wirelessly connected with via base stations, comprising:

authenticating the first mobile station with user-to-user data exchange during call set up or during a call;

constructing and sending a first message by the first mobile station;

receiving the first message by the second mobile station;

constructing and sending by the second mobile station, a second message;

receiving and verifying by the first mobile station, a validity of the second message;

accepting to share when information is verified valid in the first mobile station, a shared encryption key K;

constructing and sending by the first mobile station, a third message;

receiving and verifying by the second mobile station, a validity of the third message; and

accepting to share, when information is verified valid in the second mobile station, a shared encryption key K.

17. (Previously Presented) A method according to claim 16, wherein authentication data is exchanged through user-to-user signaling.

18. (Currently Amended) A method according claim 16 comprising exchanging authentication data through user-to-user signaling during a call ~~when a need occurs for an~~ requiring extra secure communication services~~during the call~~.

19. (Previously Presented) A method according to claim 16, wherein the first and second mobile stations execute a mutual authentication and key agreement protocol based on public-key cryptography.

20. (Currently Amended) A method according to claim 6 furtherto authenticate a mobile station in a mobile network, comprising:

forming and verifying messages for implementation of authentication of the mobile station with user-to-user data exchange during call set up or during a call, and key agreement procedures;

outputting for a presentation a commencement of extra secure communication services to a user of the mobile station;

validating an extra secure communication channel for the extra secure communication services; and

transmitting/receiving information as transformed to a radio waves from digital signals and vice versa.